PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2004-343764**

(43)Date of publication of application : **02.12.2004**

(51)Int.Cl. **H04Q 7/38**
G09C 1/00
H04L 9/32

(21)Application number : **2004-144252**

(22)Date of filing : **14.05.2004**

(71)Applicant : **LUCENT TECHNOL INC**

(72)Inventor : **PATEL SARVAR**

(30)Priority

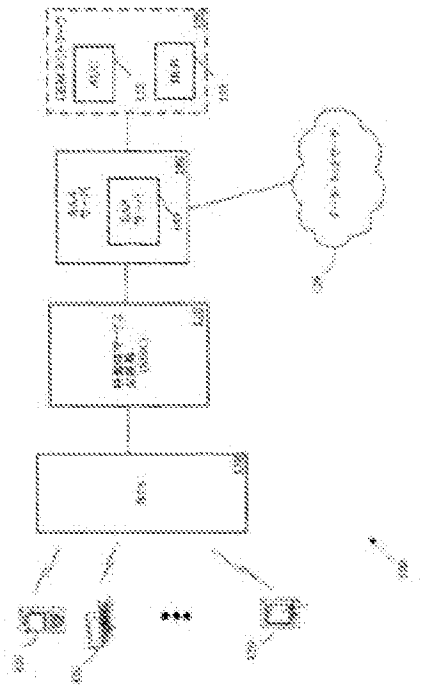
Priority number : **2003 438686** Priority date : **15.05.2003** Priority country : **US**

(54) EXECUTION OF AUTHENTICATION WITHIN COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and apparatus for executing authentication within a communication system.

SOLUTION: The method includes the steps of receiving an authentication request which contains first and second random calls from a server, and comparing the first random call with the second random call. The method further includes the steps of: denying the authentication request in response to the determination that the first random call is substantially the same as the second random call; and transmitting an encoded value to the server in response to the determination that the first random call is different from the second random call, the encoded value being generated on the basis of the first and second random calls and a key which is not shared with the server.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-343764
(P2004-343764A)
(43)公開日　平成16年12月2日(2004.12.2)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04Q	7/38	H04B	7/26	109S	5J104
G09C	1/00	G09C	1/00	640E	5K067
H04L	9/32	H04L	9/00	675A	

審査請求 未請求　請求項の数 10　OL　（全 13 頁）

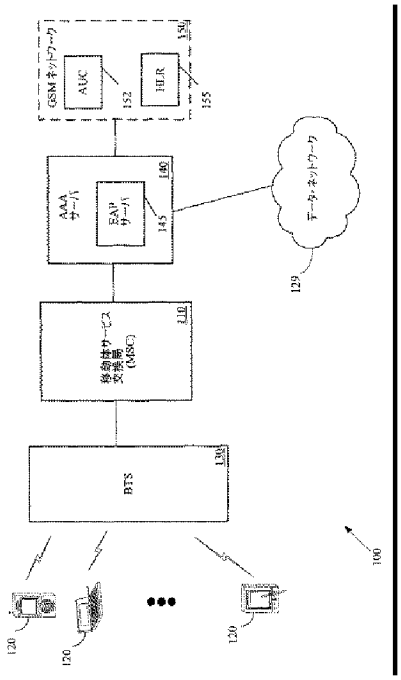
(21)出願番号　特願2004-144252 (P2004-144252)
(22)出願日　平成16年5月14日 (2004.5.14)
(31)優先権主張番号　10/438686
(32)優先日　平成15年5月15日 (2003.5.15)
(33)優先権主張国　米国 (US)

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．０７９７４－０６３６　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100106703
弁理士　産形　和央
(74)代理人　100096943
弁理士　臼井　伸一

最終頁に続く

(54)【発明の名称】通信システム内での認証の実行

(57)【要約】
【課題】通信システム内で認証を実行する方法および装置を提供すること。
【解決手段】前記方法はサーバからの第１および第２のランダムな呼び掛けを含む認証要求を受信する工程と、前記第１のランダムな呼び掛けと前記第２のランダムな呼び掛けとを比較する工程とを含む。前記方法は、前記第１のランダムな呼び掛けが実質的に前記第２のランダムな呼び掛けと同一であると決定したことに応答して前記認証要求を拒否する工程と、前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと異なると決定したことに応答して前記サーバに符号化された値を送信する工程であって、前記符号化された値は前記第１および前記第２のランダムな呼び掛けと前記サーバと共有されない鍵とに基づいて生成される工程とをさらに含む。
【選択図】図１



【特許請求の範囲】
【請求項1】
通信システム内で認証を実行する方法であって、
サーバからの第１および第２のランダムな呼び掛けを含む認証要求を受信する工程と、
前記第１のランダムな呼び掛けと前記第２のランダムな呼び掛けとを比較する工程と、
前記第１のランダムな呼び掛けが実質的に前記第２のランダムな呼び掛けと同一であると決定したことに応答して前記認証要求を拒否する工程及び、
前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと異なると決定したことに応答して前記サーバに符号化された値を送信する工程であって、前記符号化された値は前記第１および前記第２のランダムな呼び掛けと前記サーバと共有されない鍵とに基づいて生成される工程からなる方法。
【請求項2】
前記認証要求を拒否する工程が、前記認証要求に応答しない工程、サーバからの要求を拒否する工程及び、音声およびデータ通信の少なくとも１つのセッションを確立し、前記セッションを終了する工程の少なくとも１つを実行する工程からなる請求項１に記載の方法。
【請求項3】
前記サーバへの最初のランダムな呼び掛けに応答して、前記第１のランダムな呼び掛けと前記第２のランダムな呼び掛けの少なくとも１つに対応するメッセージ認証コードを受信する工程からなる請求項１に記載の方法。
【請求項4】
前記受信したメッセージ認証コードが有効かどうかを検証する工程及び、前記メッセージ認証コードが有効であると決定したことに応答して通信セッションを確立する工程からなる請求項３に記載の方法。
【請求項5】
前記受信したメッセージ認証コードを検証する工程が、
前記第１のランダムな呼び掛けと前記第２のランダムな呼び掛けとに対応する１つまたは複数の暗号鍵に基づいてマスタ鍵を決定する工程、
前記マスタ鍵に基づいてメッセージ認証コードを計算する工程及び、
前記計算されたメッセージ認証コードと前記受信したメッセージ認証コードとを比較する工程からなる請求項４に記載の方法。
【請求項6】
前記認証要求を受信する工程が、第３のランダムな呼び掛けを含む前記認証要求を受信する工程からなり、前記認証要求を拒否する工程が、前記受信したランダムな呼び掛けのいずれか２つが実質的に同一である場合に前記要求を拒否する工程からなる請求項５に記載の方法。
【請求項7】
通信システム内で認証を実行する装置であって、
サーバからの第１および第２のランダムな呼び掛けを含む認証要求を受信するように構成された受信機及び、
前記受信機に通信可能に接続され、前記第１のランダムな呼び掛けと前記第２のランダムな呼び掛けとを比較し、
前記第１のランダムな呼び掛けが実質的に前記第２のランダムな呼び掛けと同一であると決定したことに応答して前記認証要求を拒否し、
前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと異なると決定したことに応答して前記サーバに符号化された値を送信するように構成された制御装置からなり、前記符号化された値が前記第１および前記第２のランダムな呼び掛けと前記サーバと共有されない鍵とに基づいて生成される装置。
【請求項8】
前記制御装置が前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと等し

くないという判定に基づいて前記認証要求を無視するか、前記制御装置が前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと等しくないという判定に基づいて前記サーバからの前記要求を拒否するか、前記制御装置が前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと等しくないという判定に基づいて音声およびデータ通信の少なくとも１つのセッションを確立し、前記セッションを終了するか、その少なくとも１つを実行するように構成された請求項７に記載の装置。

【請求項9】

前記制御装置が前記第１のランダムな呼び掛け及び前記第２のランダムな呼び掛けに対応するメッセージ認証コードを受信するように構成された請求項８に記載の装置。

【請求項10】

アクセス端末に送信する１つまたは複数の呼び掛けを決定する工程及び、

前記１つまたは複数の呼び掛けについてメッセージ認証コード値を決定する工程であって、

前記１つまたは複数の呼び掛けの各々に対応する暗号鍵を決定する工程と、

前記１つまたは複数の呼び掛けの各々に対応する署名付き応答を決定する工程と、

前記暗号鍵の１つまたは複数と前記署名付き応答とに基づいてマスタ鍵を決定し、前記メッセージ認証コードを決定する工程とを含む工程及び、

前記１つまたは複数の呼び掛けと前記認証コードとを前記アクセス端末に送信する工程からなる方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、一般に通信システムに関し、特に無線通信システム内での認証の実行に関する。

【背景技術】

【0002】

成り済ましと盗聴は無線通信の安全に対する潜在的な脅威である。無線リンクを介した通信を適切に保護するには、まず通信機器を認証し、次いで通信内容を暗号化することが望ましい。近年、リモート当事者の識別を認証するためのいくつかの周知のプロトコルがさまざまな標準化機関によって提案されている。最近検討されているそのようなプロトコルの１つが、Ｇｌｏｂａｌ　Ｓｙｓｔｅｍ　ｆｏｒ　Ｍｏｂｉｌｅ（ＧＳＭ）加入者識別モジュール（ＳＩＭ）を用いて認証およびセッション鍵の配布を実行する拡張認証プロトコルである。以下、このプロトコルをＥＡＰ－ＳＩＭプロトコルと呼ぶ。

【0003】

ＥＡＰ－ＳＩＭプロトコルは、既存のＧｌｏｂａｌ　Ｓｙｓｔｅｍ　ｆｏｒ　Ｍｏｂｉｌｅの通信認証手順の拡張提案に基づく。ＥＡＰ－ＳＩＭプロトコルは、ＧＳＭシステムの識別モジュールを用いた相互認証およびセッション鍵のための機構を指定する。相互認証のためには、アプリケーション機能を実行する前に、クライアントとサーバはそれぞれの同一性を互いに証明しなければならない。相互認証の基本原則はいずれの当事者も同一性が証明されるまで相手を「信用」してはならないということである。

【0004】

ＧＳＭネットワークは呼び掛け－応答の機構に基づく。ＧＳＭネットワークは移動局に１２８ビットのランダムな数字（ＲＡＮＤ）呼び掛けを送信する。移動局は個別の加入者認証鍵（K_i）を用いたランダムな数字（ＲＡＮＤ）に基づいて３２ビットの署名付き応答（ＳＲＥＳ）と６４ビット暗号鍵K_cとを計算する。次いで移動局は当該ＳＲＥＳをＧＳＭネットワークに送出する。移動局からＳＲＥＳを受信すると、ＧＳＭネットワークは計算を繰り返して移動局の識別を確認する。ただし、個別の加入者認証鍵（K_i）は無線チャネル上で送信されない。個別の加入者認証鍵（K_i）は移動局とサービス網のデータベース内に存在する。受信したＳＲＥＳが計算値と一致すれば、移動局は成功裏に認証され、通信を続行できる。値が一致しないと、接続は終了し、認証の失敗が移動局に通知さ

れる。
【非特許文献1】「インターネット・プロトコル」と題するコメント要求（ＲＦＣ）７９１、１９８１年９月
【非特許文献2】「インターネット・プロトコル、バージョン６（ＩＰｖ６）仕様」と題するＲＦＣ２４６０、１９９８年１２月
【非特許文献3】Ｈ．Ｋｒａｗｃｚｙｋ、Ｍ．Ｂｅｌｌａｒｅ、Ｒ．Ｃａｎｅｔｔｉ、「Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ　ｆｏｒ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ」、ＲＦＣ２１０４、１９９７年2月
【非特許文献4】「Ｓｅｃｕｒｅ　Ｈａｓｈ　Ｓｔａｎｄａｒｄ」と題する連邦情報処理標準（ＦＩＰＳ）出版物１８０－１、Ｎａｔｉｏｎａｌ　Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｓｔａｎｄａｒｄｓ　ａｎｄ　Ｔｅｃｈｎｏｌｏｇｙ、１９９５年4月17日
【発明の開示】
【発明が解決しようとする課題】
【0005】
上記のように、ＧＳＭネットワークは１回のＲＡＮＤ呼び掛けを用いて移動局の識別を認証する。ＥＡＰ－ＳＩＭプロトコルは、ＧＳＭプロトコルの認証手順に基づいて、６４ビット暗号鍵K_cを用いた相互認証の機構を規定する。ただし、６４ビット鍵に基づいて相互認証を実行することでは、例えば、９６ビットまたは１２８ビット鍵を使用した場合には得られるはずの所望の機密保護レベルが提供されないことがある。より安全な認証の機構を提供するため、ＥＡＰ－ＳＩＭプロトコルは最大３回のＲＡＮＤ呼び掛けを規定し、その結果、認証手順に最大３つの６４ビット鍵K_cを使用できる。この３つの６４ビット鍵を組み合わせると、１９２ビット鍵になり、機密保護が強化されると思われる。ただし、複数の暗号鍵を組み合わせるだけでは必ずしも機密保護は強化されない。これは成り済ました者（すなわち非良心的な当事者）は６４ビット鍵の値を正しく推測することに基づいて移動局の認証に成功する場合があるからである。これはＥＡＰ－ＳＩＭプロトコルでは３回のセットのうち１回ごとのＲＡＮＤ呼び掛けが一意である（各K_c鍵も一意である）ことは要求されないからである。成り済ました者はこうして無権限のセッションを確立し、それによってまず単一の６４ビット鍵を正しく推測し、次いでその鍵の複数の複製を用いて移動局に対して自己を認証することで移動局との完全通話を続行することができる。
本発明は上記の１つまたは複数の問題の影響を克服するかまたは少なくとも軽減することを目的とする。
【課題を解決するための手段】
【0006】
本発明の一実施形態では、通信システム内で認証を実行する方法が提供される。前記方法はサーバからの第１および第２のランダムな呼び掛けを含む認証要求を受信する工程と、前記第１のランダムな呼び掛けと前記第２のランダムな呼び掛けとを比較する工程とを含む。前記方法は、前記第１のランダムな呼び掛けが実質的に前記第２のランダムな呼び掛けと同一であると決定したことに応答して前記認証要求を拒否する工程と、前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと異なると決定したことに応答して前記サーバに符号化された値を送信する工程であって、前記符号化された値は前記第１および前記第２のランダムな呼び掛けと前記サーバと共有されない鍵とに基づいて生成される工程とをさらに含む。
【0007】
本発明の一実施形態では、通信システム内で認証を実行する装置が提供される。前記装置はサーバからの第１および第２のランダムな呼び掛けを含む認証要求を受信するように構成された受信機を含む。前記装置は前記受信機に通信可能に接続された制御装置を含む。前記制御装置は、前記第１のランダムな呼び掛けと前記第２のランダムな呼び掛けとを比較し、前記第１のランダムな呼び掛けが実質的に前記第２のランダムな呼び掛けと同一であると決定したことに応答して前記認証要求を拒否するように構成されている。前記制

御装置はさらに、前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと異なると決定したことに応答して前記サーバに符号化された値を送信するように構成され、前記符号化された値は前記第１および前記第２のランダムな呼び掛けと前記サーバと共有されない鍵とに基づいて生成される。

【0008】

本発明の一実施形態では、認証を実行するシステムが提供される。前記システムは複数の呼び掛けと、前記複数の呼び掛けのうち少なくとも第１および第２の呼び掛けを含む認証要求を送信するように構成されたサーバからはアクセスできない鍵に基づいて生成された複数の対応する値とにアクセスする。前記システムは、前記第１のランダムな呼び掛けと前記第２のランダムな呼び掛けとを比較し、前記第１のランダムな呼び掛けが実質的に前記第２のランダムな呼び掛けと同一であると決定したことに応答して前記認証要求を拒否する装置を含む。前記装置は前記第１のランダムな呼び掛けが前記第２のランダムな呼び掛けと異なると決定したことに応答して前記サーバに符号化された値を送信するように構成され、前記符号化された値は前記第１および前記第２のランダムな呼び掛けと前記秘密鍵とに対応する値の少なくとも一部に基づく。

【0009】

本発明の一実施形態では、通信システム内で認証を実行する方法が提供される。前記方法はアクセス端末に送信する１つまたは複数の呼び掛けを決定する工程と、前記１つまたは複数の呼び掛けについてのメッセージ識別認証コード値を決定する工程とを含む。前記少なくとも１つまたは複数の呼び掛けについての前記メッセージ認証コード値は前記１つまたは複数の呼び掛けの各々に対応する暗号鍵を決定する工程と、前記１つまたは複数の呼び掛けの各々に対応する署名付き応答を決定する工程と、前記暗号鍵の１つまたは複数と前記署名付き応答とに基づいてマスタ鍵を決定し、メッセージ認証コードを決定する工程とを含む。前記少なくとも１つまたは複数の呼び掛けについての前記メッセージ認証コード値はさらに、前記１つまたは複数の呼び掛けと前記認証コードとを前記アクセス端末に送信する工程を含む。

【0010】

本発明は添付図面と共に以下の説明を参照することで理解できよう。前記図面では同一の要素には同一の参照番号が付与されている。

本発明についてさまざまな変更を加えることができ、別の実施形態も可能であるが、本発明の特定の実施形態を図面に例示し以下に詳述する。ただし、前記特定の実施形態についての本明細書の説明は本発明を開示された特定の実施形態を限定するものではなく、逆に、添付の特許請求の範囲に記載する本発明の精神と範囲を逸脱しない限り、本発明はすべての変更、等価形態、および代替形態を含むものである。

【発明を実施するための最良の形態】

【0011】

本発明の実施例について以下に説明する。話を分かりやすくするために、本明細書では実際の実施形態のすべての特徴を網羅しているわけではない。当然ながら、そのような任意の実際の実施形態を開発する過程で、開発者の特定の目標を達成するために、実施形態ごとに異なるシステム関連およびビジネス関連の制約の準拠などの数多くの実施形態固有の決定をしなければならないことは理解されるであろう。さらに、そのような開発努力は複雑で時間がかかる場合があるが、それにもかかわらず本発明の恩恵を享受する当業者にとっては日常的な作業であることを理解されたい。

【0012】

図面、特に図１を参照すると、本発明の一実施形態による通信システム１００が示されている。図を見やすくするために、図１の通信システム１００内の認証はＥＡＰ－ＳＩＭプロトコルに従って実行される。ただし、本発明の精神と範囲を逸脱しない限り、別の実施形態では他の認証プロトコルを使用できることを理解されたい。ＥＡＰ－ＳＩＭプロトコルのインターネット草案（２００３年２月）がインターネット技術特別調査委員会によって利用可能になっている（ｈｔｔｐ：／／ｗｗｗ．ｗａｔｅｒｓｐｒｉｎｇｓ．ｏｒｇ

／ｐｕｂ／ｉｄ／ｄｒａｆｔ－ｈａｖｅｒｉｎｅｎ－ｐｐｐｅｘｔ－ｅａｐ－ｓｉｍ－１０．ｔｘｔを参照）。

【0013】

図１の通信システムは１つまたは複数のアクセス端末１２０が１つまたは複数の基地局（ＢＴＳ）によってインターネットなどのデータ・ネットワーク１２９と通信できるようにする移動体サービス交換局１１０を含む。図１の移動体サービス交換局１１０は一般に複製、通信、ランタイム、およびシステム管理サービスを提供する。移動体サービス交換局１１０は通話経路の設定および終了などの呼処理機能を扱うこともできる。アクセス端末１２０は、携帯電話、パーソナル・デジタル・アシスタント（ＰＤＡ）、ラップトップ・コンピュータ、デジタル・ページャ、無線カード、およびデータ・ネットワーク１２９にアクセス可能なその他の任意の装置を含むさまざまな装置の１つを含むことができる。

【0014】

図２は本発明の一実施形態によるアクセス端末１２０の例示のブロック図である。実施例では、それほど限定されていないが、アクセス端末１２０はＧＳＭ携帯電話である。アクセス端末１２０は制御装置１２２と記憶装置１２３とを含む加入者識別モジュール（ＳＩＭ）１２１を備える。図の実施形態では、ＳＩＭ１２１は以下に詳述する形で認証手順を実行する認証モジュール１２５を含む。認証モジュール１２５は、ソフトウェアで実施される場合、制御装置１２２によって実行でき、記憶装置１２３内に記憶できる。図２には示していないが、ＳＩＭ１２１は国際移動体加入者識別（ＩＭＳＩ）、個別加入者認証鍵（K_i）、暗号化鍵生成アルゴリズム（Ａ８）、および個人識別番号（ＰＩＮ）を含むことができる。図示の実施形態のアクセス端末１２０は無線リンク上でデータを送受信する送受信論理１２６とアンテナ１２７とを含む。

【0015】

再び図１を参照すると、通信システム１００は、認証、許可、およびアカウンティング（ＡＡＡ）サーバ１４０に接続された移動体サービス交換局１１０を含む。図の実施形態では、ＡＡＡサーバ１４０はＥＡＰサーバ１４５を含むが、別の実施形態では、ＥＡＰサーバ１４５をスタンドアロン装置内で実施できる。ＥＡＰサーバ１４５はＧＳＭネットワーク１５０とのインタフェースをとり、データ・ネットワーク１２９とＧＳＭネットワーク１５０との間のゲートウェイとして動作する。ＧＳＭネットワーク１５０は移動体サービス交換局１１０に、各々がランダムな（ＲＡＮＤ）呼び掛け（例えばランダムな数字）、署名付き応答（ＳＲＥＳ）、および暗号鍵（K_c）を含む１つまたは複数のトリプレットを提供する。一実施形態では、ＲＡＮＤは１２８ビットのランダムな数字で、個別加入者認証鍵K_i（最大１２８ビット長）と併用して、それぞれ６４ビット、３２ビット長の暗号鍵K_cとＳＲＥＳ値とを生成する。

【0016】

以下に詳述するように、本発明の１つまたは複数の実施形態では、アクセス端末１２０とＥＡＰサーバ１４５との間で相互認証を実行する改良型方式が提供される。本発明の一実施形態では、通信システム１００内で実施される相互認証手順は、いくつかの既存のプロトコルに基づいて得られるものより優れたセキュリティを提供する。

【0017】

図１に示すデータ・ネットワーク１２９はインターネット・プロトコル（ＩＰ）に準拠するデータ・ネットワークなどのパケット交換データ・ネットワークであってもよい。ＩＰの１つのバージョンが「インターネット・プロトコル」と題するコメント要求（ＲＦＣ）７９１、１９８１年９月に記載されている。別の実施形態では、ＩＰｖ６などのＩＰの他のバージョンまたはその他のコネクションレス方式のパケット交換標準も使用できる。ＩＰｖ６の１つのバージョンが「インターネット・プロトコル、バージョン６（ＩＰｖ６）仕様」と題するＲＦＣ２４６０、１９９８年１２月に記載されている。別の実施形態では、データ・ネットワーク１２９は他のタイプのパケットベースのデータ・ネットワークを含んでいてもよい。そのようなその他のパケットベースのデータ・ネットワークは例えば非同期転送モード（ＡＴＭ）、フレーム・リレー・ネットワークなどを含む。

【0018】
本明細書で使用する「データ・ネットワーク」は、１つまたは複数の通信ネットワーク、チャネル、リンクまたは経路、およびそのようなネットワーク、チャネル、リンクまたは接続経路上でデータをルーティングするために使用されるシステムまたは装置（ルータなどの）を指すことができる。
【0019】
図１の通信システム１００の構成は本質的に例示的なもので、通信システム１００のその他の実施形態で構成要素の数を増減してもよい。例えば、ＧＳＭネットワーク１５０は認証センタ（ＡｕＣ）１５２で生成されるトリプレットのセットを記憶するビジタ・ロケーション・レジスタ（図示せず）を含んでいてもよい。別の例として、一実施形態では、システム１００は運用、管理、保守、およびプロビジョニング機能を提供するネットワーク管理システム（図示せず）を含んでいてもよい。さらに、移動体サービス交換局１１０およびＡＡＡサーバ１４０は別の要素として示されているが、別の実施形態では、これらの要素の機能は単一の要素で実行してもよい。
【0020】
特に述べられていない限り、または説明から明らかなように、「処理」または「演算」または「計算」または「決定」または「表示」などの用語は、コンピュータ・システムのレジスタおよびメモリ内で物理、電子量として表されるデータを操作してコンピュータ・システムのメモリまたはレジスタ、あるいはその他の情報記憶、伝送、または表示装置内で同様に物理量として表される他のデータに変換するコンピュータ・システムの動作およびプロセスを指す。
【0021】
図３を参照すると、図１の通信システム１００で採用できる認証手順の一実施形態が示されている。認証手順はＥＡＰサーバ１４５が（２０５で）識別要求をアクセス端末１２０に提供する動作で開始する。アクセス端末１２０は（２１０で）アクセス端末１２０を一意に識別する識別子で応答する。例えば、アクセス端末１２０は国際移動体加入者識別（ＩＭＳＩ）または一時的識別（ペンネーム）を含む識別子を提供してもよい。
【0022】
アクセス端末１２０が（２１０で）提供する応答に続けて、アクセス端末１２０は（２１５で）ＥＡＰサーバ１４５から起動要求を受信する。アクセス端末１２０は受信した起動要求に（２２０で）応答する。開始要求と開始応答によって、アクセス端末１２０とＥＡＰサーバ１４５は両当事者がサポートするプロトコルのバージョンについて打ち合わせる。特に、ＥＡＰサーバ１４５から（２１５で）提供される起動要求はＥＡＰサーバ１４５がサポートするバージョン・リストを示すＶｅｒｓｉｏｎ＿Ｌｉｓｔ属性を含む。次いで、アクセス端末１２０が（２２０で）提供する起動応答はアクセス端末１２０が選択するバージョン番号を含むバージョン属性を含む。またその起動応答に乗せて（２２０で）、アクセス端末１２０は最初の呼び掛けの$RAND_c$をＥＡＰサーバ１４５に送信する。
【0023】
アクセス端末１２０から（２２０で）起動要求を受信すると、ＥＡＰサーバ１４５はＧＳＭネットワーク１５０の認証センタ（ＡｕＣ）１５２から１つまたは複数のＧＳＭトリプレットを取得する。場合によっては、ＧＳＭトリプレットは将来使用することを見越してＥＡＰサーバ１４５が事前取得してもよい。ＥＡＰ－ＳＩＭプロトコルでは認証実行時に最大３つのトリプレットの使用をサポートしている。上記のように、各トリプレットはランダムな（ＲＡＮＤ）呼び掛け、署名付き応答（ＳＲＥＳ）、および暗号鍵（K_c）を含み、ＳＲＥＳとK_cはＲＡＮＤ値とK_i鍵に基づいて計算される。ＥＡＰサーバ１４５は異なるトリプレットのＲＡＮＤ呼び掛けが異なることを規定する。
【0024】
次いで、ＥＡＰサーバ１４５は（２２５で）アクセス端末１２０に呼び掛け要求を送信する。呼び掛け要求は１つまたは複数のＲＡＮＤ呼び掛けとＲＡＮＤ呼び掛けに対応するメッセージ認証コードMAC_kとを含む。ＭＡＣ値を計算するアルゴリズムは当業で周知

である。ＭＡＣ値を計算するアルゴリズムの一例は、Ｈ．Ｋｒａｗｃｚｙｋ、Ｍ．Ｂｅｌｌａｒｅ、Ｒ．Ｃａｎｅｔｔｉ、「Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ　ｆｏｒ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ」、ＲＦＣ２１０４、１９９７年２月と題する参考文献に記載されている。

【0025】

図３に示す認証手順では、MAC_kは受信したトリプレットのＲＡＮＤ値とアクセス端末１２０から（２２０で）前もって送信された）$RAND_c$に基づいて計算される。例えば、ＥＡＰサーバ１４５が２つのＲＡＮＤ（Ｒ１およびＲ２）呼び掛けを送信するとした場合、MAC_kは少なくともＲ１、Ｒ２および$RAND_c$に基づいて計算される。ＥＡＰ－ＳＩＭプロトコルはＭＡＣ値の計算の前に認証鍵ｋが必要であると規定する。認証鍵ｋを計算するには、マスタ鍵（ＭＫ）を先に計算する必要がある。ＭＫは以下の式（１）に基づいて計算できる。

【0026】

$$MK = SHA[\ldots, \text{暗号鍵}(K_{c1}, K_{c2}, K_{c3}), RAND_c, \ldots] \quad (1)$$

上式で、ＳＡＨは安全なハッシュ・アルゴリズムを表し、暗号鍵はＧＳＭの一部で、$RAND_c$はアクセス端末１２０が提供する最初の呼び掛けである。安全なハッシュ・アルゴリズムの一例は、「Ｓｅｃｕｒｅ　Ｈａｓｈ　Ｓｔａｎｄａｒｄ」と題する連邦情報処理標準（ＦＩＰＳ）出版物１８０－１、Ｎａｔｉｏｎａｌ　Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｓｔａｎｄａｒｄｓ　ａｎｄ　Ｔｅｃｈｎｏｌｏｇｙ、１９９５年４月１７日に記載されている。

【0027】

ＭＡＣ値とマスタ鍵は他のタイプの情報（例えば、バージョン番号、識別など）に基づいて計算することもできる。ただし、図を見やすくし、本発明の実施形態を必要以上に複雑にしないために、本明細書では詳細は割愛する。

【0028】

マスタ鍵（ＭＫ）が上式（１）を用いて計算されると、擬似乱数関数（ＰＲＦ）に提供され、認証鍵ｋが生成される。上記のように、認証鍵ｋはＭＡＣ値の計算に必要である。使用できる擬似乱数関数の一例は、Ｈ．Ｋｒａｗｃｚｙｋ、Ｍ．Ｂｅｌｌａｒｅ、Ｒ．Ｃａｎｅｔｔｉ、「Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ　ｆｏｒ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ」、ＲＦＣ２１０４、１９９７年２月に記載されている。

【0029】

認証鍵ｋが計算されると、ＥＡＰサーバ１４５は少なくともアクセス端末１２０に送信するＲＡＮＤ呼び掛け（すなわち、受信したＧＳＭトリプレットの$RAND_c$およびＲＡＮＤ番号）に基づいてＭＡＣ値を決定する。計算されたＭＡＣ値は、１つまたは複数のＧＳＭトリプレットのＲＡＮＤ呼び掛けと共に、（２２５で）アクセス端末１２０に送信される。

【0030】

アクセス端末１２０の認証モジュール１２５（図２を参照）は（２２７で）移動体サービス交換局１１０（図１参照）とのセッションが確立されたかどうかを判定し、受信したＲＡＮＤ呼び掛けとＭＡＣ値とに基づいてデータ・ネットワーク１２９にアクセスする。アクセス端末１２０がＥＡＰサーバ１４５を認証することが可能であればセッションを確立することができる。下記のように、本発明の一実施形態では、受信したＭＡＣ値が有効であると決定した後で、また、受信したＲＡＮＤ呼び掛けのいずれの２つも同一（または実質的に同一）ではないと決定した後で、アクセス端末１２０はセッションを確立する。

【0031】

アクセス端末１２０はＥＡＰサーバ１４５から送信されたＲＡＮＤ呼び掛けのそのＭＡＣ値を別に計算し、次いで、計算したＭＡＣ値を受信したＭＡＣ値と比較することで受信したＭＡＣ値の有効性を検証する。アクセス端末１２０は初期の鍵K_iを使用できるので、アクセス端末１２０ＥＡＰサーバ１４５が計算するのと同様にＭＡＣ値を計算できる。

ＥＡＰ－ＳＩＭプロトコルでは、アクセス端末１２０は受信したＭＡＣ値が有効であるとの判定に基づいてＥＡＰサーバ１４５を認証できる。ただし、受信したＭＡＣ値の有効性に基づく認証は限定された機密保護しか提供しないことがある。これは、成り済ました者が６４ビットのK_C鍵の値を正しく推測してアクセス端末１２０とのセッションを確立する可能性があるからである。すなわち、K_Cの値を正しく推測することで、成り済ました者はマスタ鍵（ＭＫ）を計算して認証鍵ｋを引き出し、今度はそれを用いてＭＡＣ値を決定することができる。成り済ました者はＭＡＣ値をアクセス端末１２０に送信して自らを認証し、その後、アクセス端末１２０と無権限の会話を完全に行う。さらに、ＥＡＰ－ＳＩＭプロトコルによって許される複数のＧＳＭトリプレットの複数のＲＡＮＤ呼び掛けを送信することにより、認証手順がより安全になるとは必ずしもいえない。これは、ＲＡＮＤ呼び掛けの各々が一意でなければならないという制約がないためである。したがって、成り済ました者は所与のＲＡＮＤ呼び掛けについてK_Cの値を正しく推測し、K_Cの複数の複製に基づいてマスタ鍵を計算し、マスタ鍵に基づいて有効なＭＡＣ値を計算することができる。

【0032】

無権限のアクセスの可能性を減らすために、本明細書に２つの実施形態を記載する。第１の実施形態は本発明の一実施形態の図３のブロック２２７の流れ図を示す図４に示されている。図を見やすくするために、ＥＡＰサーバ１４５は認証のために複数のＲＡＮＤ呼び掛けと、これらのＲＡＮＤ呼び掛けの１つのＭＡＣ値を送信するものとする。図４を参照すると、認証モジュール１２５（図２を参照）は受信したＲＡＮＤ呼び掛けのうちいずれか２つが同一であるかどうかを（４０５で）判定する。ＲＡＮＤ呼び掛けのうちいずれの２つも同一でない場合（言い換えれば、ＲＡＮＤ呼び掛けがすべて一意であれば）、認証モジュール１２５はＥＡＰサーバ１４５から受信したＭＡＣ値が有効かどうかを（４１０で）判定する。上記のように、アクセス端末１２０はＥＡＰサーバ１４５から送信されたＲＡＮＤ呼び掛けのそのＭＡＣ値を別に計算し、計算したＭＡＣ値を受信したＭＡＣ値と比較することで受信したＭＡＣ値の有効性を検証する（４１０で）ことができる。２つのＭＡＣ値が一致しない場合、アクセス端末１２０は（４１２で）ＥＡＰサーバ１４５から受信した（図３の参照番号２２５を参照）呼び掛け要求を無視する。規定の時間内に有効なＭＡＣ値を受信しなかった場合、認証は失敗し、接続は確立されない。

【0033】

受信したＭＡＣ値が有効であると認証モジュール１２５が（４１０で）判定すると、認証モジュール１２５は受信したＲＡＮＤ呼び掛けに基づいてＳＲＥＳ値を（４１５で）計算し、次いでＳＲＥＳ値の中のＭＡＣ値を決定する。別の実施形態では、認証モジュール１２５は、暗号鍵、ＲＡＮＤ呼び掛けなどの他の情報に基づいてＭＡＣ値を決定できる。次いでＭＡＣ値は応答－呼び掛けパケット（図３の参照番号２３０を参照）内でＥＡＰサーバ１４５に（４１７で）送信される。アクセス端末１２０からＭＡＣ値を受信したＥＡＰサーバ１４５は、ＭＡＣ値の有効性を検証し、ＭＡＣ値が有効と判定された場合、アクセス端末１２０に成功信号（図３の参照番号２４５を参照）を送信する。成功信号を受信すると、認証モジュール１２５はアクセス端末１２０と移動体サービス交換局（１１０、図を参照）との間に（４２０で）セッションを確立する。

【0034】

ＥＡＰサーバ１４５から受信した複数のＭＡＣ値のうち少なくとも２つが同一であると認証モジュール１２５が（４０５で）判定した場合、認証モジュール１２５はアクセス端末１２０との間にセッションを確立する前に一意の有効なＲＡＮＤ呼び掛けを送信するようにＥＡＰサーバ１４５に要求する。ＲＡＮＤ呼び掛けの各々が一意であることを要求することで、非良心的な当事者は少なくとも２つの異なる値（例えば、K_c鍵）を正しく推測してアクセス端末１２０とのセッションを確立しなければならないため、認証手順はより安全になる。

【0035】

ＥＡＰサーバ１４５からのＭＡＣ値が一意でないと（４０５で）判定されると、認証モ

ジュール１２５はいくつかの方法の１つでＥＡＰに新しいＲＡＮＤ呼び掛けを送信させる。一実施形態では、認証モジュール１２５はＥＡＰサーバ１４５からの呼び掛け要求（図３の参照番号２２５を参照）を（４２５で）無視することができる。事前選択された時間が満了すると、ＥＡＰサーバ１４５は新しいＲＡＮＤ呼び掛けとそれに対応するＭＡＣ値とを送信できる。別の実施形態では、認証モジュール１２５はＥＡＰサーバ１４５からの呼び掛け要求を（４３０で）拒否し、さらにＥＡＰサーバ１４５に新しいＲＡＮＤ呼び掛けとそれに対応するＭＡＣ値とを送信させることができる。さらに別の実施形態では、認証モジュール１２５はアクセス端末１２０との間で（４３５で）セッションを確立させ、その後接続を終了し、したがってＥＡＰサーバ１４５に新しいＲＡＮＤ呼び掛けとそれに対応するＭＡＣ値とを送信させることができる。

【0036】

このように、本発明の１つまたは複数の実施形態によれば、受信したＲＡＮＤ呼び掛けの各々が互いに異なることをアクセス端末が要求する場合には認証手順がより安全になる。この手法は、提案されたＥＡＰ－ＳＩＭプロトコルに大幅な変更を加えず、または全く変更を加えずにＥＡＰ－ＳＩＭプロトコルの状況において採用できる。図３の認証手順を確実にする別の実施形態は、署名付き応答（ＳＲＥＳ）をマスタ鍵（ＭＫ）の計算の一部とすることを要求することを含む。したがって、上記の式（１）を以下のように式（２）として書き直すことができる。

$$MK = SHA[\ldots, \text{暗号鍵}(K_{c1}, K_{c2}, K_{c3}), SRES_1, SRES_2, SRES_3, RAND_c, \ldots] \quad (2)$$

【0037】

ＳＲＥＳ値を含むようにマスタ鍵を定義すると、非良心的な当事者はK_cだけでなくＳＲＥＳ値の正しい値を推測しなければならないので認証はより安全になる。式（２）はＥＡＰサーバ１４５が３つのＧＳＭトリプレッツを使用する（K_{c1}、K_{c2}、K_{c3}、$SRES_1$、$SRES_2$、および$SRES_3$の各項があるため）ことを前提にするが、この式は単一のトリプレットまたは任意の他の数のトリプレットで使用するように容易に変更できる。ＭＫを計算するために式（２）を使用すると、１つのトリプレット（したがって、１つのＲＡＮＤ呼び掛け）しか使用しなくても認証はより安全になる。これは敵がK_cの値だけでなくＳＲＥＳ値も正確に予測しなければならないからである。ＭＫの計算を変更するこの別の実施形態では、ＥＡＰ－ＳＩＭプロトコルがマスタ鍵の計算のためのアルゴリズムを定義する限り、ＥＡＰ－ＳＩＭプロトコルを変更する必要がある。

【0038】

一実施形態では、図３および図４の認証手順で式（１）の代わりに式（２）を使用してもよい。すなわち、一実施形態では、認証手順はマスタ鍵の計算にＳＲＥＳ値を含ませる（式（２）に示すように）ことができ、さらに、ＥＡＰサーバ１４５に複数のＧＳＰトリプレットを使用する場合に一意のＲＡＮＤ呼び掛けを送信させる手順を含ませることもできる。

【0039】

図３は相互認証手順を示すが、本発明の１つまたは複数の上記の実施形態が一方的認証手順にも適用できることを理解されたい。片務的認証手順では、ＥＡＰサーバ１４５は、例えば、アクセス端末１２０に１つまたは複数のＲＡＮＤ呼び掛けを送信し、アクセス端末１２０が受信したＲＡＮＤ呼び掛けに応答することでアクセス端末１２０を認証することができる。

【0040】

例示するために、本発明の１つまたは複数の実施形態を無線通信システムの状況で述べている。ただし、別の実施形態では、本発明を有線ネットワークで実施することもできることを理解されたい。さらに、本発明は音声専用通信または音声およびデータ通信をサポートするシステムに適用可能である。

【0041】

本明細書のさまざまな実施形態で例示したさまざまなシステム層、ルーチン、またはモ

ジュールは実行可能な制御装置（図２の制御装置１２２など）であってもよいことは当業者には明らかであろう。制御装置１２２はマイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ、プロセッサ・カード（１つまたは複数のマイクロプロセッサまたはマイクロコントローラを含む）、またはその他の制御もしくは演算装置を含むことができる。本明細書で言及した記憶装置はデータおよび命令を記憶する１つまたは複数のマシン可読記憶媒体を含むことができる。記憶媒体は、動的または静的ランダム・アクセス・メモリ（ＤＲＡＭまたはＳＲＡＭ）、消去可能なプログラマブル読み出し専用メモリ（ＥＥＰＲＯＭ）、電気的に消去可能なプログラマブル読み出し専用メモリ（ＥＥＰＲＯＭ）およびフラッシュ・メモリなどの半導体メモリ・デバイス、固定、フロッピー（登録商標）、着脱式ディスク、テープなどのその他の磁気媒体、およびコンパクト・ディスク（ＣＤ）またはデジタル・ビデオ・ディスク（ＤＶＤ）などの異なる形態のメモリを含むことができる。さまざまなシステム内でさまざまなソフトウェア層、ルーチン、またはモジュールを構成する命令はそれぞれの記憶装置内に記憶できる。命令がそれぞれの制御装置１２２によって実行されると、対応するシステムはプログラミングされた処理を実行する。

【0042】

上記で開示されている特定の実施形態は例示的なものにすぎない。本発明は本明細書の教示の恩恵にあずかる当業者には明らかな、異なったまたは均等な形で変更し、実施することができる。さらに、本明細書に示す詳細な構成または設計は特許請求の範囲に記載する場合を除いて限定されない。したがって、上記で開示した特定の実施形態は改変および変更ができ、そのような変形形態はすべて本発明の範囲と精神を逸脱するものではないことは明らかである。したがって、本明細書で述べた保護策は特許請求の範囲に記載する。

【図面の簡単な説明】

【0043】

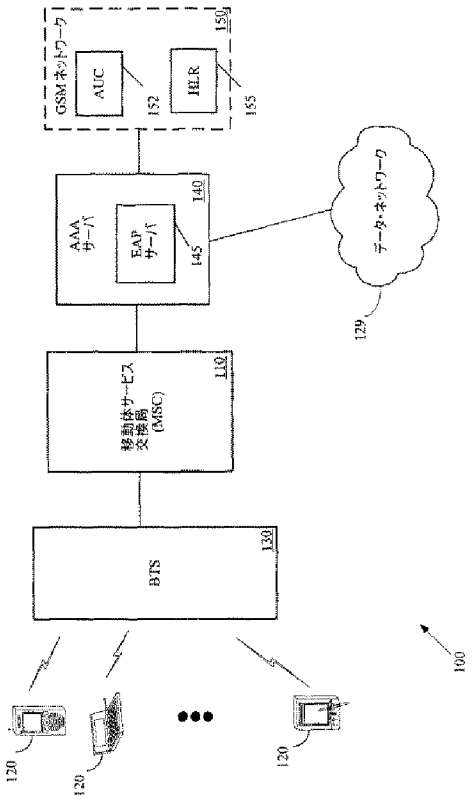
【図1】本発明の一実施形態による通信システムのブロック図である。

【図2】本発明の一実施形態によるアクセス端末のブロック図である。

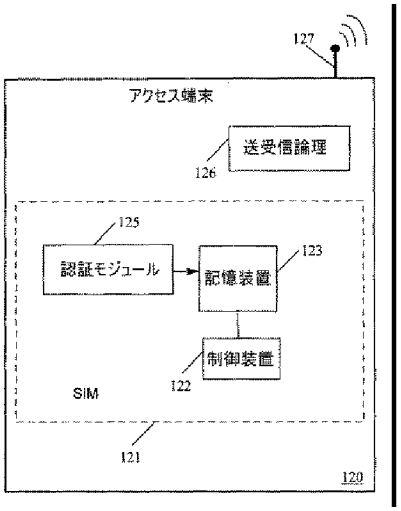
【図3】本発明の一実施形態による、図１の通信システム内で実行される認証手順の例示的なメッセージの流れ図である。

【図4】本発明の一実施形態による、図１の通信システム内で採用できる方法の流れ図である。

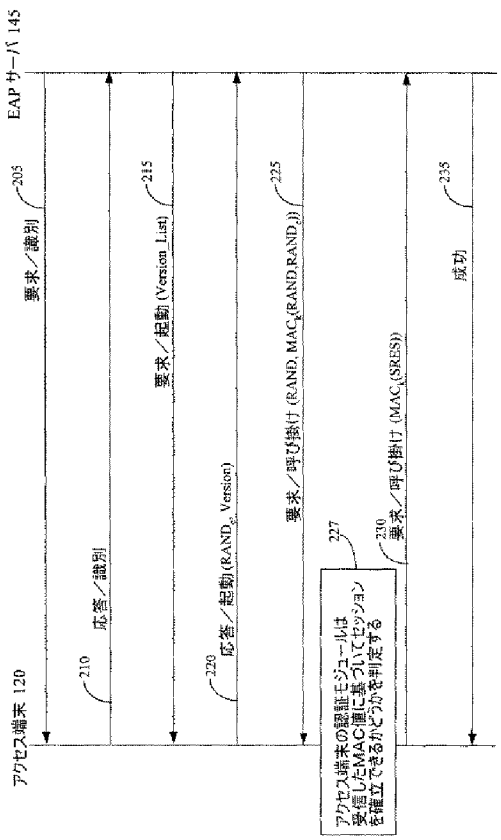
【図1】


GSMネットワーク
150
AUC
152
IMEI
155
AAA
サーバ
140
EAP
サーバ
145
データ・ネットワーク
129
移動体サービス
交換機
(MSC)
110
BTS
130
100
120
120
120

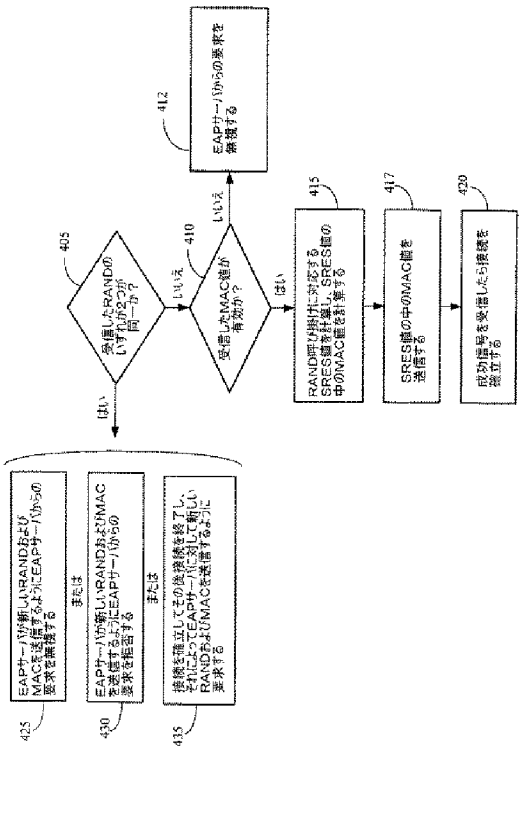
【図2】


127
アクセス端末
送受信論理
126
125
認証モジュール
123
記憶装置
制御装置
122
SIM
121
120

【図3】


EAP サーバ 145
アクセス端末 120
要求／識別
205
210
応答／識別
要求／起動 (Version_List)
215
220
応答／起動(RAND, Version)
要求／呼び掛け (RAND, MAC(RAND,RAND))
225
227
アクセス端末の認証モジュールは
受信したMACに基づいてセッション
を確立できるかどうかを判定する
230
要求／呼び掛け (MAC (SRES))
成功
235

【図4】


405
受信したRANDの
いずれかが
同一か？
はい
いいえ
410
受信したMACが
有効か？
いいえ
はい
412
EAPサーバからの要求を
構築する
415
RAND呼び掛けに対応する
SRES値を計算し、SRES値の
中のMAC値を計算する
417
SRES値の中のMAC値を
送信する
420
成功信号を受信したら接続を
設立する
425
EAPサーバからRANDおよび
MACを送信するようにEAPサーバからの
要求を構築する
または
430
EAPサーバからRANDおよびMAC
を受信するようにEAPサーバからの
要求を指定する
または
435
接続を確立してその後接続を終了し、
再びこのEAPサーバに接続するときに
RANDおよびMACを送信するように
要求する

(74)代理人　100101498
弁理士　越智　隆夫
(74)代理人　100096688
弁理士　本宮　照久
(74)代理人　100104352
弁理士　朝日　伸光
(74)代理人　100128657
弁理士　三山　勝巳
(72)発明者　サーヴァー　パテル
アメリカ合衆国　０７０４５　ニュージャーシィ，モントヴィル，ミラー　レーン　３４

Ｆターム(参考) 5J104 AA07　KA02　KA05　KA06　NA02　NA38　PA01
5K067 AA32　BB04　DD13　DD24　EE02　EE10　EE23　HH22　HH24　HH36